ITrust
IT Security Services

COMMENT RENDRE VISIBLE LA SÉCURITÉ

ITrust est
un acteur innovant
dans la surveillance et
l'amélioration continue
de la Sécurité des Systèmes d'Information.

Constat du marché

Firewall/Proxy + Antivirus = Protection complète

- **3 entreprises sur 4 se sont faites pirater au cours des deux dernières années.**

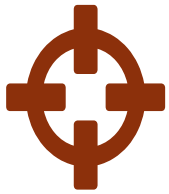
- **6 entreprises françaises sur 10 ont subi au moins 1 incident de sécurité en 2011, dont 5 ont subi des pertes financières (source : PWC 2011).**

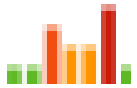
- **Dans 20% des cas, les entreprises mettent plus d'une semaine pour revenir à une situation normale.**

- **8 entreprises sur 10, qui subissent une intrusion ou une attaque, ne le savent pas.**

Le « bon » Tableau de bord

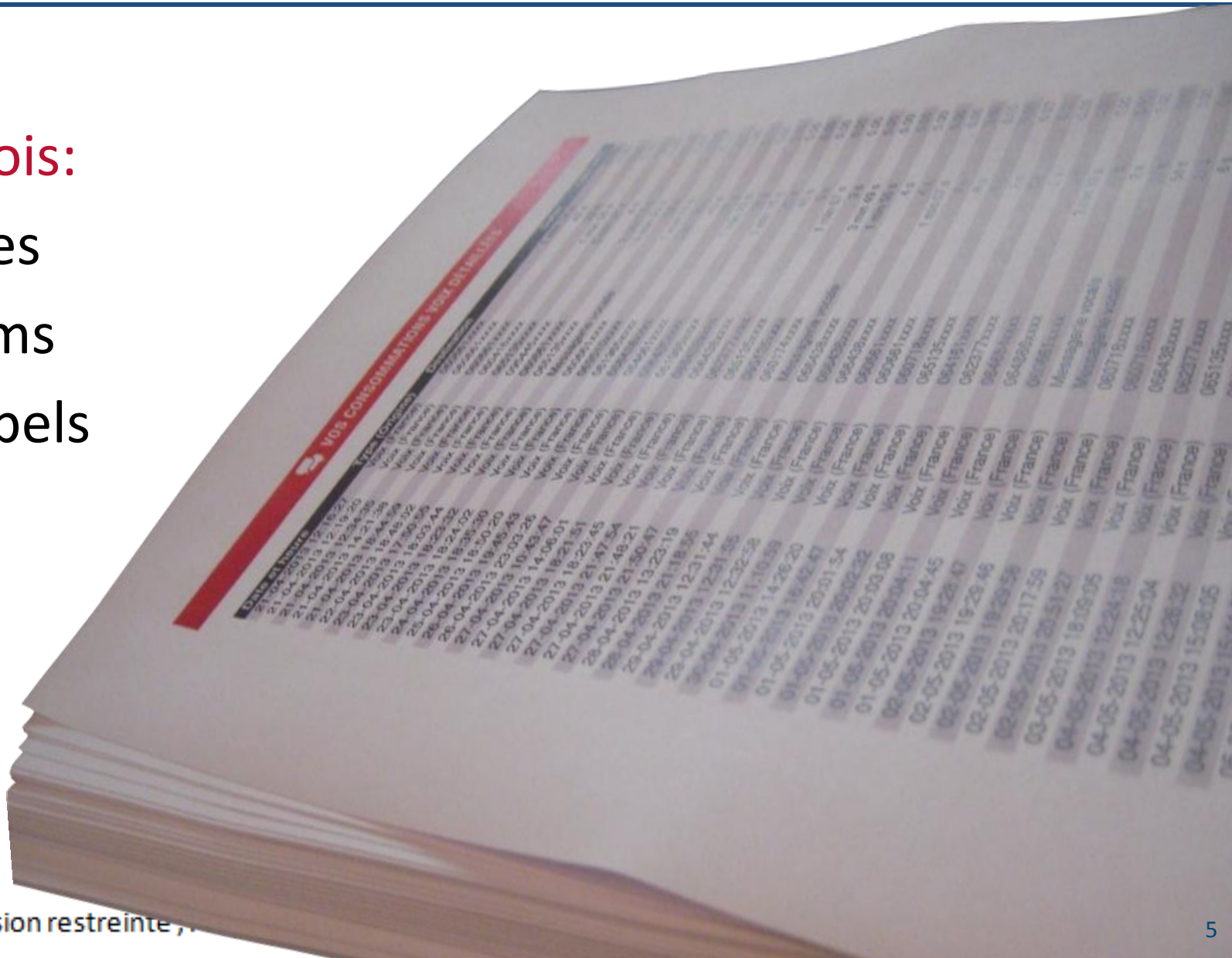
1. **Les indicateurs « utiles »:**
   - **compréhension de la situation**
   - **pilotage vers les buts**
   - **répartition des rôles: leviers actionnables**
2. **Une visualisation efficace:**
   - **adaptée à l'auditoire**
   - **mise en contexte**
   - **qui utilise l'œil comme un co-processeur**





Le Big Data domestique: la facture téléphone des ados

- En 3 mois:
- 98 pages
- 5543 sms
- 214 appels



La question: l'usage est il raisonnable ?

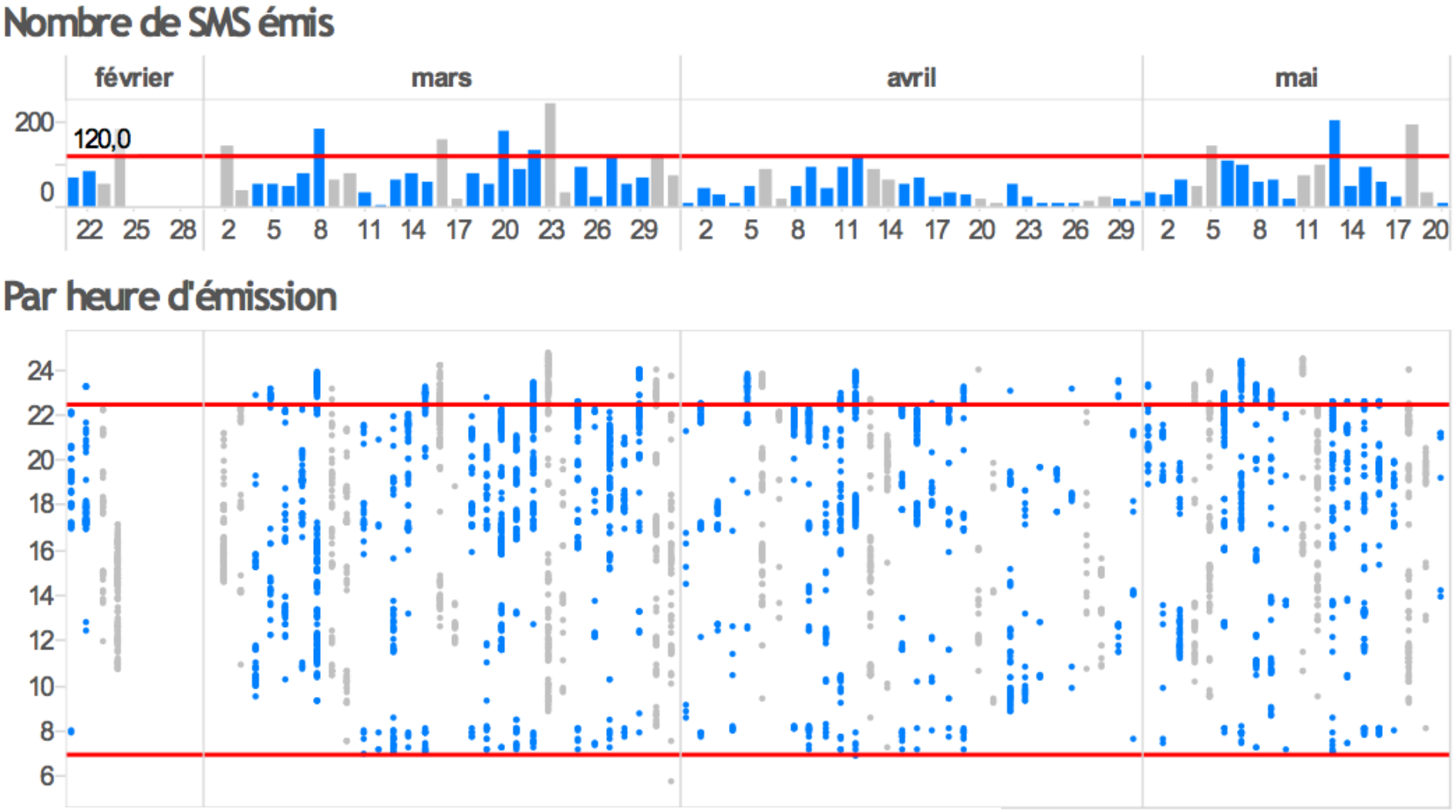


Tableau de bord de la sécurité

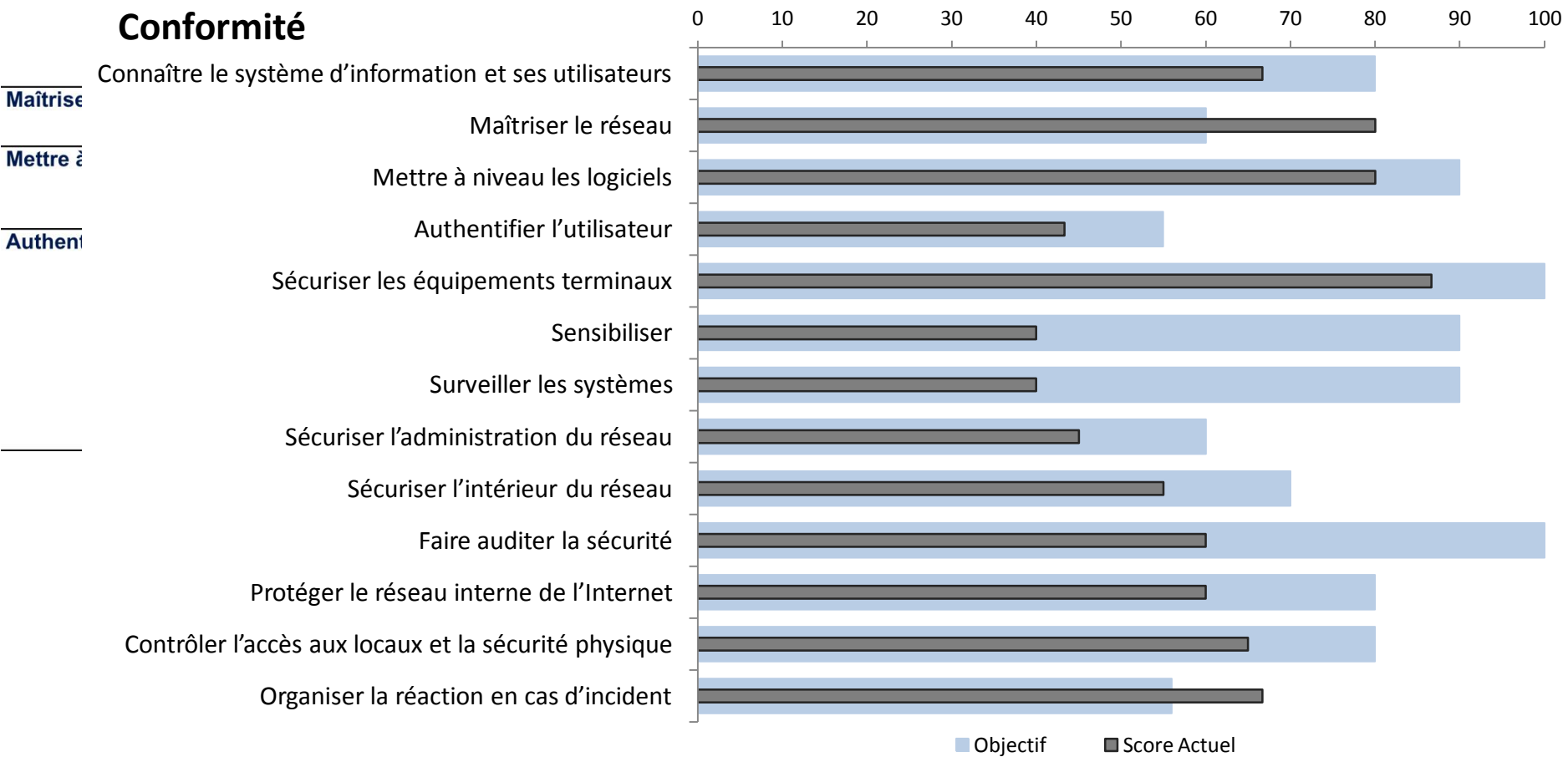
ITrust
IT Security Services

Quelles sont les questions ?

- Quelles mesures faut il prendre ?
- Sont elles correctement appliquées?
- Est ce efficace ?

Voir la Conformité à un référentiel

Thème	Questionnaire ANSSI V1.0 Janvier 2013	0 à 5 ou Non Applicable
Connaître le système d'information et ses utilisateurs	Disposer d'une cartographie précise de l'installation informatique et la maintenir à jour	NA



☑ Découverte automatique

Manager vos machines, services, et applications

☑ Audits de vulnérabilité

Réduisez votre exposition à des attaques.

Augmentez votre niveau de sécurité.

☑ Tendances de sécurité

Evaluez les efforts et le ROI de vos actions,

Identifiez les risques de sécurité à l'avance.

☑ Alertes de sécurité ciblées

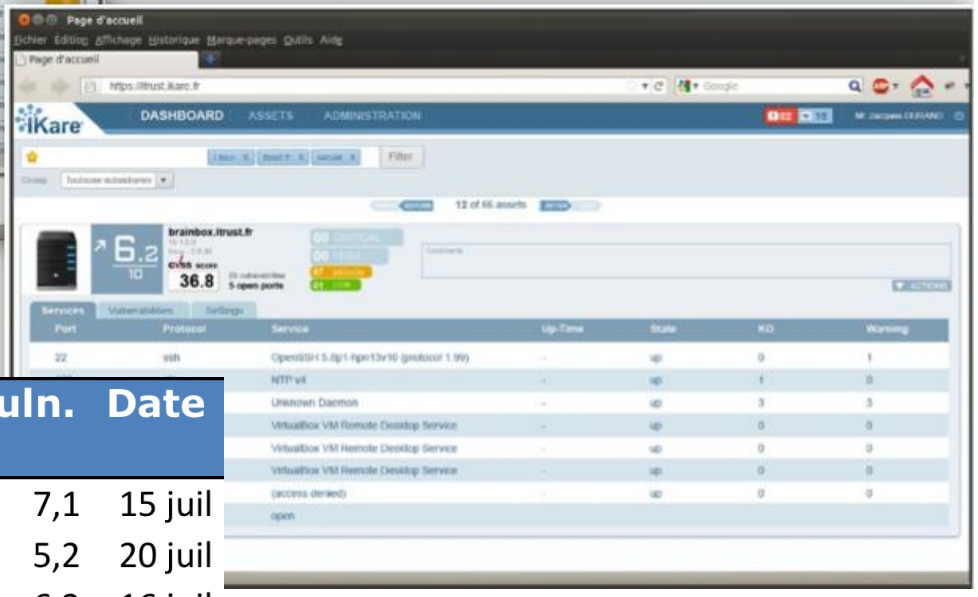
Facilite le travail de maintenance opérationnelle

☑Rapports compréhensibles

Rapports détaillés lisibles par le management et les opérationnels

IKare découvre automatiquement les machines du réseau

Chaque machine reçoit une note
10 – sans vulnérabilité connue
0 – sans aucune protection



Chaque détail est accessible

Nom	IP	Vuln.	Date
vsg-82a46-115	192.168.146.115	7,1	15 juil
macomp192168176222	192.168.176.222	5,2	20 juil
macomp192168151222	192.168.151.222	6,2	16 juil
macomp192168151232	192.168.151.232	8,3	21 juil
macomp192168176232	192.168.176.232	9,6	16 juil
vsg-82a46-111	192.168.146.111	7,2	17 juil

Une synthèse peut être exportée

Voir l'inventaire des machines

Nom	Fonction	Vuln.	Age	Prop	D	I	C	Exig.
vsg-82a46-115	Serveur Droits Active Directory	7,1	6	sophie.laforet@masociete.fr	3	3	1	7
macomp192168176222	Bureautique comptabilité Lyon	5,2	1	albert.durand@masociete.fr	1	2	3	6
macomp192168151222	Base de données clients Lyon	6,2	5	albert.durand@masociete.fr	3	1	1	5
macomp192168151232	Base de données clients Paris	8,3	0	albert.durand@masociete.fr	3	1	1	5
macomp192168176232	Bureautique comptabilité Paris	9,6	5	albert.durand@masociete.fr	1	2	2	5
vsg-82a46-111	Serveur Sécurité surveillance	7,2	4	sophie.laforet@masociete.fr	2	1	2	5
macomp192168179222	Base des stocks	7,1	0	brigitte.lafont@masociete.fr	1	2	1	4
vm146s02	Contrôle d'accès badgeuse	9,0	7	remi.dupont@masociete.fr	2	1	1	4
macomp192168152232	Cluster bureautique de secours	8,1	6	brigitte.lafont@masociete.fr	2	1	1	4
vsg-84a46-107	Serveur développement Web	7,5	5	sophie.laforet@masociete.fr	1	1	1	3
macomp192168179232	Base des transactions Secours	8,8	5	brigitte.lafont@masociete.fr	1	1	1	3

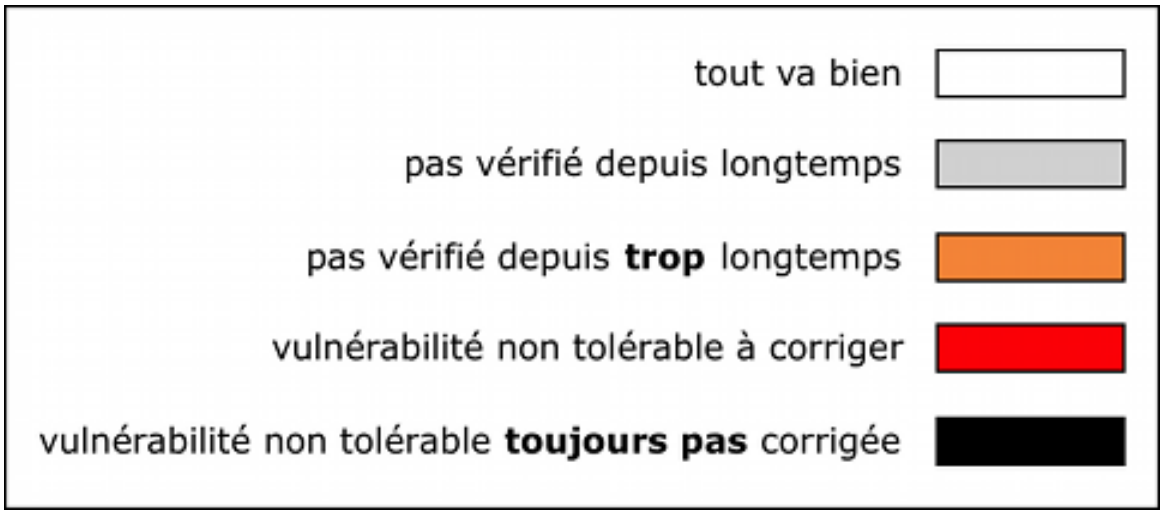
Il est possible d'associer des informations quelconques aux machines

Les nouvelles machines découvertes apparaissent comme de nouvelles lignes

Voir la gestion des vulnérabilités

La situation est préoccupante si:

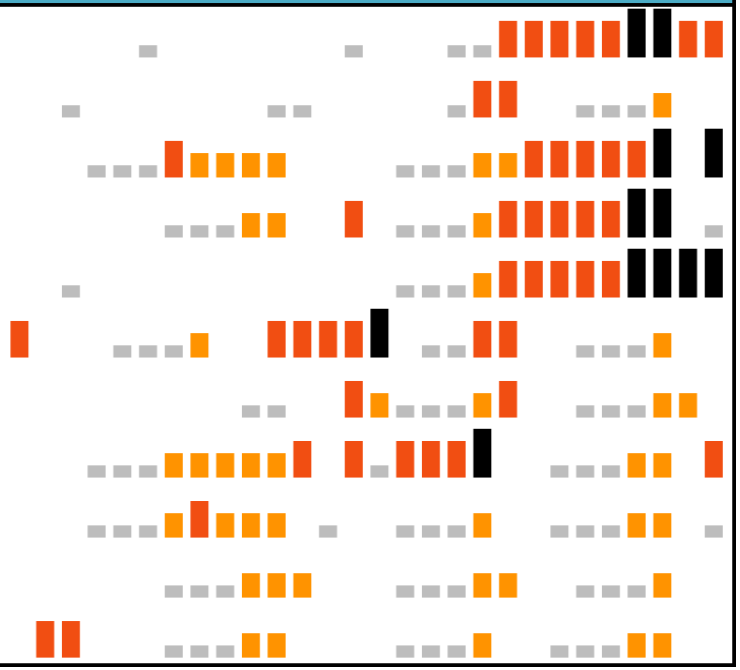
1. une vulnérabilité est présente
2. aucune vérification n'a été faite depuis longtemps



Voir la gestion des vulnérabilités

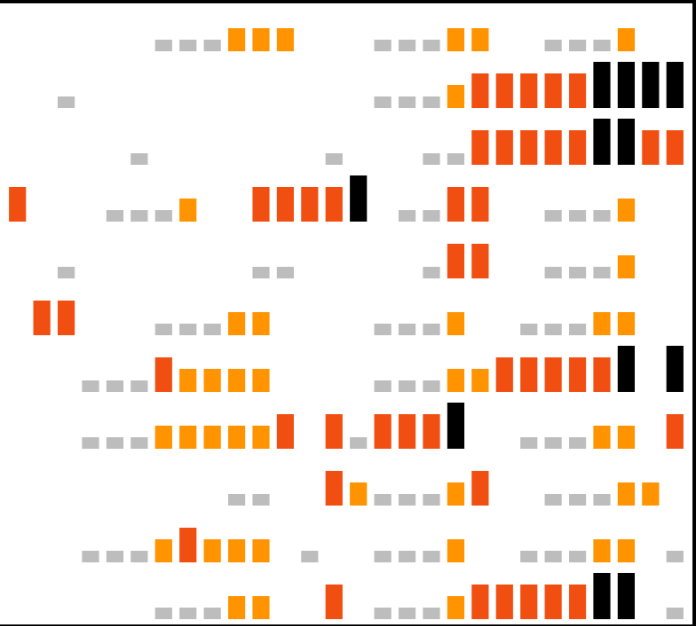
ITrust
IT Security Services

ok	pas vérifié depuis longtemps	pas vérifié depuis trop longtemps	vulnérabilité non tolérable	vulnérabilité non tolérable toujours pas corrigée

Etat	Ce que fait la machine	Historique (4 semaines glissantes)
●	Base de données clients Lyon	
	Base de données clients Paris	
●	Base des stocks	
●	Base des transactions Secours	
●	Bureautique comptabilité Lyon	
	Bureautique comptabilité Paris	
	Cluster bureautique de secours	
●	Contrôle d'accès badgeuse	
●	Serveur développement Web	
	Serveur Droits Active Directory	
	Serveur Sécurité surveillance	

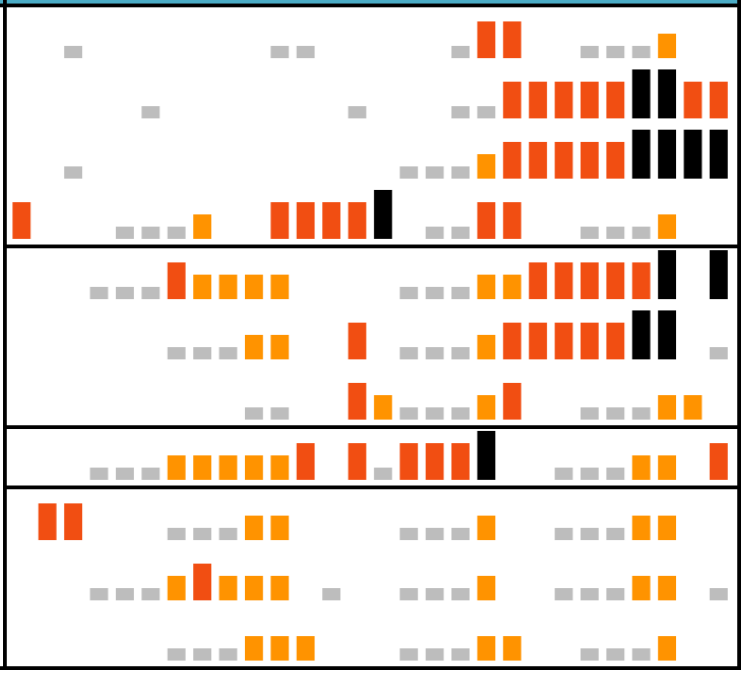
Voir croisement Criticité/ Vulnérabilité

Exig.	Etat	Ce que fait la machine	Historique (4 semaines glissantes)
7		Serveur Droits Active Directory	
6		Bureautique comptabilité Lyon	
5		Base de données clients Lyon	
5		Bureautique comptabilité Paris	
5		Base de données clients Paris	
5		Serveur Sécurité surveillance	
4		Base des stocks	
4		Contrôle d'accès badgeuse	
4		Cluster bureautique de secours	
3		Serveur développement Web	
3		Base des transactions Secours	



Voir qui doit agir

Prop.	IP	Etat	Historique (4 semaines glissantes)
albert.durand@masociete.fr	192.168.151.232		
	192.168.151.222		
	192.168.176.222		
	192.168.176.232		
brigitte.lafont@masociete.fr	192.168.179.222		
	192.168.179.232		
	192.168.152.232		
remi.dupont@masociete.fr	192.168.146.228		
sophie.laforet@masociete.fr	192.168.146.111		
	192.168.146.107		
	192.168.146.115		



Vulnérabilités des fonctions essentielles

Groupes	Etat	Historique (4 semaines glissantes)	Ce que fait la machine
Comptabilité	●		Bureautique comptabilité Lyon
			Bureautique comptabilité Paris
Développement			Cluster bureautique de secours
			Serveur développement Web
Sécurité			Serveur Sécurité surveillance
			Serveur Droits Active Directory
			Contrôle d'accès badgeuse
Ventes	●		Base des transactions Secours
			Base des stocks
			Base de données clients Lyon
			Base de données clients Paris

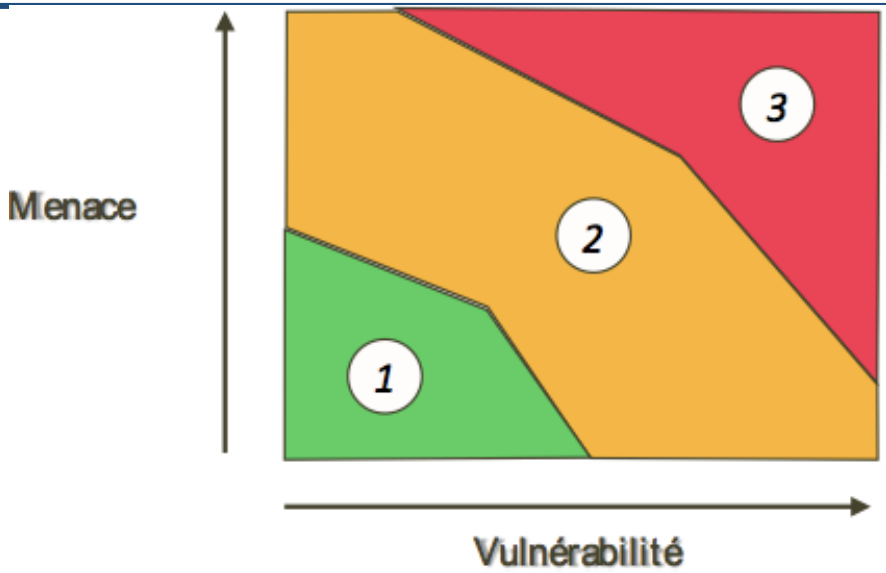
Il est possible de moduler la tolérance aux vulnérabilités par groupe

Une machine présente dans plusieurs groupes les « affecte » tous

Voir les risques

Echelle de risques (Conséquence X Exposition)

- **3** Conséquences graves et exposition forte
- **2** Conséquences et exposition moyenne
- **1** Conséquences et exposition faibles



publicité de non-conformité et 150k€

2 ans de prison et 30k€

50k€ / heure indisponible

Famille	Risque	E	Fonction
Confidentialité	Accès non autorisé		Gestion des droits
Juridique	Godfrain		Authentification des accès
Perte Image	Altération site web		Publication site web
Perte exploitation	Indisponiblité Bureautique		Production et secours
	Indisponiblité Base de données		
Perte financière	Fraude		Facturation

Conclusion

Rendre visible la sécurité pour :

- Surveiller les vulnérabilités en temps réel

- Vérifier le respect
  - des intervalles de surveillance
  - des délais de corrections critiques

- Démontrer les pratiques et la conformité

Contact

ITrust - Siège Social
55 Avenue l'Occitane,
BP 67303
31673 Labège Cedex

+33 (0)5.67.34.67.80
contact@itrust.fr
www.itrust.fr
www.ikare-monitoring.com